



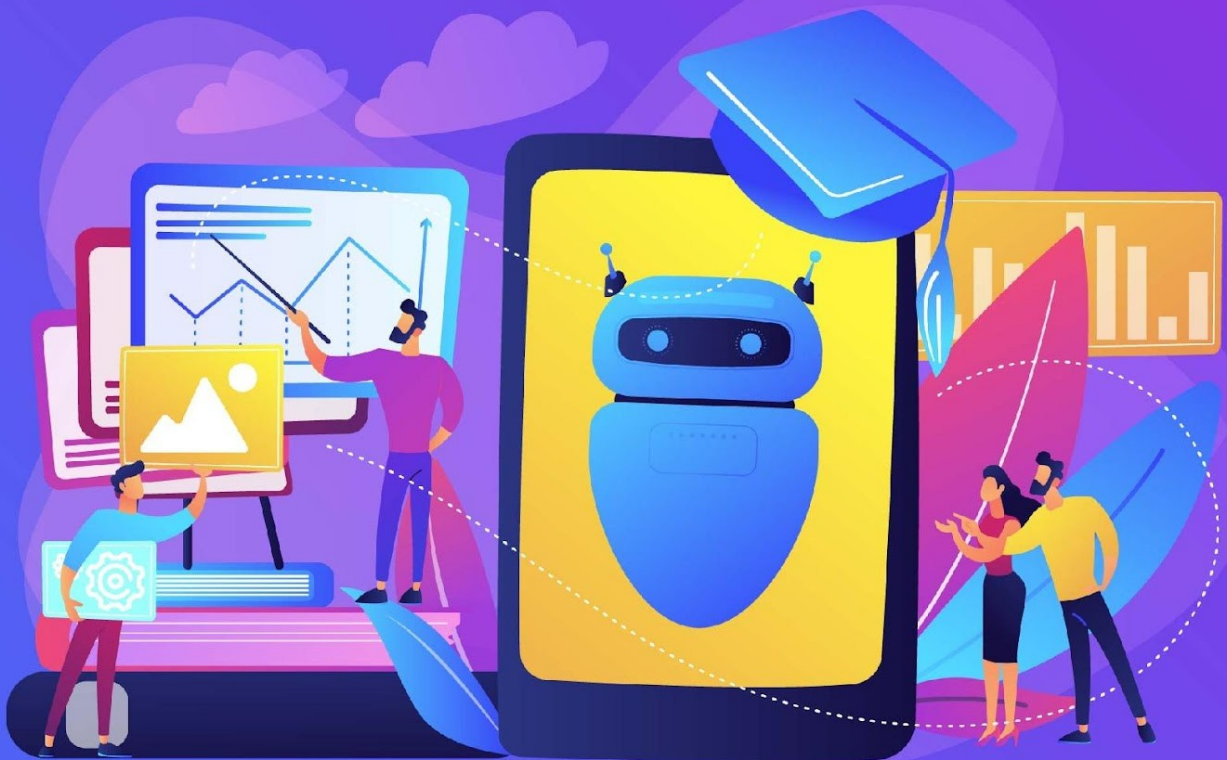
Navigating AI Regulations:  
Practical Guide

Project Number:  
2024-2-DE02-KA210-VET-000287096

---

Training Program

# AI-Driven Creativity: Advanced Training for Digital Innovators



Co-funded by  
the European Union

# Training Program

## AI-Driven Creativity: Advanced Training for Digital Innovators

### Module 4

## Data Governance for AI in the Creative Industry

### Navigating AI Regulations: Practical Guide

Project Number: 2024-2-DE02-KA210-VET-000287096

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Document Name	Module 4: Data Governance for AI in the Creative Industry
Project Activity	Activity 2: Producing the Training Program 'AI-Driven Creativity: Advanced Training for Digital Innovators'
Revision Type	Final
Revision Date	30.06.2025
Authors	INI-Novation (Germany), Budakov Films (Bulgaria)

### Declaration on copyright:



This document is protected through the Creative Commons Attribution-Non-Commercial-Share-Alike 4.0 International License. You are free to:

- Share — copy and redistribute the material in any medium or format
- Adapt — remix, transform, and build upon the material under the following terms:
- Attribution — you must give appropriate credit, provide a link to the license, and indicate if changes are made. You may do so in any reasonable manner, but not in any way that suggests the licensor endorses you or your use.
- Non-commercial — You may not use the material for commercial purposes.
- Share Alike — If you remix, transform, or build upon the material, you must distribute your contributions under the same license as the original.

Any unauthorized use or reproduction of the contents of this training module will be considered a violation of copyright law and subject to legal action.

# Contents

1. About the Training Program	5
2. Unlock the Full Potential of Your Training: Tips for the Learners	5
2.1. Mastering Effective Content Gathering	5
2.2. Setting Your Own Self-Paced Learning Rhythm	5
2.3. Consistent Structure Aligned with EQF Level 3 Competencies	7
3. Composition and Presentation of Learning Module 4 “Data Governance for AI in the Creative Industry”	7
3.1. Introduction	7
3.2. Goals and Learning Objectives	8
3.3. Content	8
3.4. Conclusion	14
3.5. Practical Exercises	15
3.6. Assessment Criteria	17
3.7. References	18
About the Project	19

# 1. About the Training Program

The training program “AI-Driven Creativity: Advanced Training for Digital Innovators” is a cornerstone result of the Erasmus+ co-funded project “Navigating AI Regulations: Practical Guide” (Project Number: 2024-2-DE02-KA210-VET-000287096). Tailored to meet the evolving needs of entrepreneurs in creative industries, this comprehensive initiative is designed to equip participants with the essential knowledge and skills to navigate the AI Act effectively. By covering critical aspects such as risk classification, compliance, transparency, and data governance, the program ensures that creative professionals can integrate AI into their workflows responsibly, adhere to legal standards, manage data ethically, and foster trust through transparent practices. Ultimately, this training not only raises awareness and understanding of complex regulatory landscapes but also empowers users to harness AI technologies in innovative ways, thereby enhancing their competitive edge in the digital age.

## 2. Unlock the Full Potential of Your Training: Tips for the Learners

### 2.1. Mastering Effective Content Gathering

To maximize your learning experience with our hands-on training modules, begin by reviewing the learning objectives provided by the consortium. Reflect on how these objectives relate to the specific challenges you face in your daily work routines and identify the key topics that directly impact your professional environment. Next, draw connections between the practical applications featured in each of the five modules and your real-world cases by considering concrete examples and case studies included in the training materials. Finally, organize your insights using digital tools such as note-taking apps or mind maps, ensuring that you can easily reference and integrate these concepts into your daily practices for a truly effective learning experience.

### 2.2. Setting Your Own Self-Paced Learning Rhythm

Our training modules are designed with a clear structure that includes the following parts: **Introduction, Goals and Learning Objectives, Content, Conclusion, Practical Exercises, and Assessment Criteria** for self-evaluation.

To maximize your learning experience, here are five tips:

- First, thoroughly review the **Introduction** to understand the context of each module.
- Second, clearly grasp the **Goals and Learning Objectives** to align your personal learning targets with the module's focus.
- Third, actively engage with the **Content** by taking detailed notes and relating new information to your daily work challenges.
- Fourth, reflect on the **Conclusion** to consolidate your understanding and draw actionable insights.
- Fifth, approach each **Practical Exercise** as a self-driven research project by using the **Assessment Criteria** to measure your progress and identify areas for improvement.

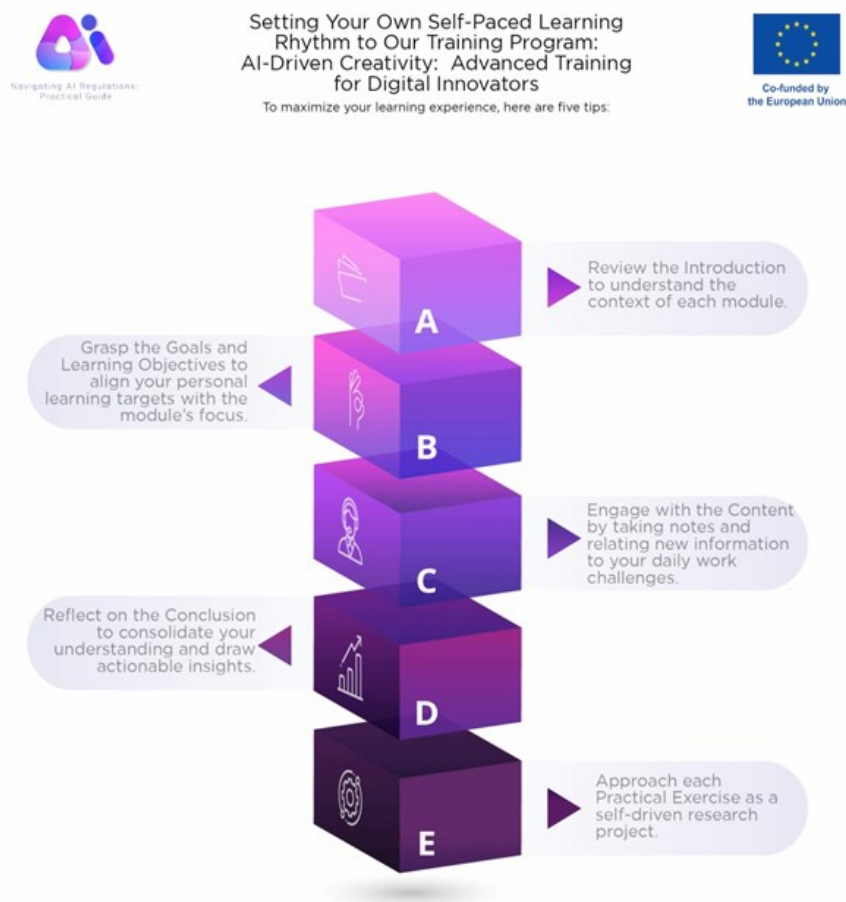


Figure 1. Image: Infographic focused on the learning tips. Source: Navigating AI Regulations Consortium

Finally, to ensure you have mastered the skills and knowledge from all five training modules, we highly encourage you to complete the final **quiz: AI-Driven Creativity Comprehensive Assessment**. The final comprehensive assessment not only reinforces your learning but also motivates you to explore all parts of the program, and please feel free to reach out to the consortium if you have any questions.

## 2.3. Consistent Structure Aligned with EQF Level 3 Competencies

Each training module is designed with a consistent structure aligned with EQF Level 3 - established during Activity 1 and detailed in the document "Competency Framework Alignment: EQF Level 3 for AI and Creative Practices," which is based on the Core Competencies for AI-Driven Creativity: Aligning with AI Act Regulations.

# 3. Composition and Presentation of Learning

## Module 4 “Data Governance for AI in the Creative Industry”

### 3.1. Introduction

Dear learners, while in Modules 1 and 2 we explored how to understand the legal requirements of the AI Act, the GDPR, and copyright regulations within the context of the creative industries, Module 4, now, provides you with essential knowledge on **data privacy, intellectual property (IP), and ethical AI**. We want to motivate you to ensure compliance with legal and regulatory frameworks - such as GDPR and copyright laws - across all stages of your AI-enhanced creative production and workflows.

As AI tools become increasingly integral to creative work, taking responsibility for compliance means more than just legal awareness. It is about building **trust, transparency, and sustainable practices**. For this purpose, we will not only guide you through the theories of data privacy, IP, and ethical AI, but also showcase real-world examples of AI compliance - highlighting how companies and professionals integrate ethical AI practices and respect referring rules and regulations.

In summary, Module 4 equips you with practical knowledge to manage data responsibly within clear regulatory guidelines, ensuring alignment with predictable data governance scenarios and helping you understand key regulatory frameworks like the GDPR and copyright laws. The flexible, user-friendly structure of this module allows you to progress at your own pace while developing and enhancing your skills. If you have any questions or need further clarification, please contact our team directly. We are here to support your learning journey and ensure you can apply the training effectively.

#### Key words:

*Data governance; GDPR; IP regulations; copyright; data security; ethical AI, compliance.*

## 3.2. Goals and Learning Objectives

Module 4, “*Data Governance for AI in the Creative Industry*”, enables creative professionals to identify key data governance principles, including data privacy, security, and ethical handling, relevant to AI-driven creative projects. Learners will be equipped to implement strategies for managing and protecting datasets used in AI applications, ensuring compliance with GDPR and related regulations.

Specifically, by completing this module, participants will:

- **Understand key data governance principles**, including data privacy, security, and ethical data management in AI-powered creative workflows.
- **Ensure compliance with GDPR and IP laws** and implement strategies for handling personal data and protecting creative assets. The module also supports creative professionals developing IP protection and valorization strategies.
- **Assess potential data security risks** by recognizing vulnerabilities in AI-powered tools and applying risk mitigation strategies to safeguard sensitive information.
- **Apply ethical data management practices**, ensuring responsible data collection, storage, and usage while maintaining transparency in AI-driven creative processes.
- **Analyze practical examples of GDPR compliance, IP protection, and ethical AI data governance** in design, branding, and content creation.

This module equips creative professionals with the tools necessary to safeguard their work, protect sensitive data, and align their AI-driven practices with evolving regulatory requirements.

## 3.3. Content

Artificial intelligence has become a true game changer also in creative industries. It automates processes, relieves the burden on sales, marketing, and customer orientation, and accelerates document processing. But with the existence of IP regulations as well as with the introduction of the GDPR and EU's new AI regulations, the pressure on companies and individuals to understand **key data governance principles** use of AI is growing. Therefore, let's start this training by taking a look into **data privacy, security, and ethical data management**.

**Data privacy** refers to the rights and practices around how personal or user-generated data is collected, stored, shared, and used, especially to ensure that individuals have control over their own information.

**Data security** means protecting digital assets (scripts, images, videos, audio, design files, etc.) from unauthorized access, leaks, or theft. For creatives, this includes both original work and any third-party content used in AI tools. It matters in creative workflows because it protects Your IP, it avoids legal trouble, and it ensures client's trust: Your art, scripts, footage, or music are valuable; if stolen or misused, you lose control and revenue. Using copyrighted content in AI training or outputs without permission can lead to lawsuits. And your clients need assurance that their confidential creative assets are handled securely.

**Ethical data management** refers to using data transparently, fairly, and with respect for people's rights. With ethical data management you ensure that AI tools and processes don't misuse or exploit data. In creative fields, this includes respecting ownership and privacy of people in your content (e.g., actors, models, clients) and avoiding unauthorized use of creative assets (stock images, artworks, music, etc.) to train or prompt AI.

Let us look at an **example** how a photographer should ethically and legally handle model consent when using facial recognition AI, which processes biometric data to identify or verify individuals. Under the GDPR, biometric data used for identification requires explicit, informed consent. It falls under special category data (Art. 9 GDPR), and it must be justified by a clear, lawful purpose. The photographer should use the following step-by-step approach to handle the consent:

1. **Explain the Purpose:** clearly inform, why facial recognition is being used (e.g., to tag photos, sort images, or apply style filters), what data will be collected (facial images, landmarks, etc.), whether the AI is third-party or in-house, and if the images or biometric data will be stored or shared.
2. **Use a Detailed Consent Form**, including a plain-language explanation of facial recognition use, a checkbox for explicit consent and the right for the model to withdraw at any time. Here is an example statement: "I consent to the use of facial recognition software to analyze and categorize my facial images. I understand that this data may be used for [specific purpose] and will not be shared without additional consent. I may withdraw this consent at any time."
3. **Offer a Clear Opt-Out:** if the model doesn't consent, ensure that the model's images are not processed by facial recognition and that an alternative workflow is available (e.g., manual tagging)
4. **Limit Data Use:** only process what is strictly needed, avoid storing full facial scans unless essential, and use hashing or encryption to protect identity
5. **Be Transparent in Your Privacy Policy:** update your privacy policy to reflect i.e. AI tools used, third-party services involved, how long biometric data is stored, and how models can access or delete their data.

Dear learners, please make sure that you **ensure compliance with GDPR and IP laws** by implementing strategies for handling personal data and protecting creative assets. The following table illustrates how to apply data security in practice:

Task	Security Practice	Creative Explanation
Uploading files to AI tools	Use only secure, GDPR-compliant platforms	Think of it like handing your art to a trusted gallery, not leaving it on a park bench.
Sharing work in progress	Use encrypted drives and cloud services with access controls	Use password-protected “view-only” links, not public folders.
Collaborating with AI models	Avoid uploading content with sensitive IP or unlicensed materials	Don’t feed AI tools with unapproved samples, brand assets, or movie clips.
Version control	Maintain secure backups and track who made changes	Like keeping drafts safe in a locked drawer, but digital.

*Table 1. How to apply data security in creative practices [1]*

In the example above, the photographer should avoid relying on verbal consent, using facial recognition by default, using images from shoots in datasets without consent and sharing data with AI tools or platforms without model awareness. These practices can be summarized in the general core compliance suggestions:

- Use licensed datasets and AI tools;
- Encrypt and watermark valuable content;
- Only collaborate on platforms with strong access control; and
- Keep logs of data sources and usage permissions.

It is of utmost importance to respect these practices and to avoid common mistakes that breach IP. Those mistakes can be i.e. using AI models trained on copyrighted art/music without verifying usage rights. It can also be sharing raw footage or unlicensed content in public AI repositories or forgetting to strip metadata from media files before sharing. Here is a suggested general process with steps and elements you should follow, when it comes to implementing strategies for handling personal data and protecting creative assets:

## Ensuring Data Governance in AI-Powered Creative Workflows

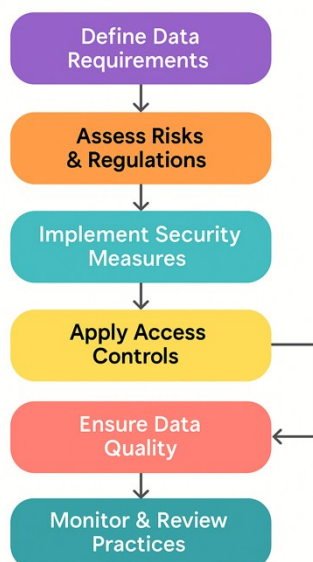


Figure 2. Ensuring Data Governance in AI-Powered Creative Workflows [©INI-Novation based on generative AI]

In conclusion, it is essential to recognize and evaluate data risks in creative AI projects. This can be accomplished by applying data governance tools to ensure ethical and legal data use and – generally spoken – by advocating for responsible AI in your creative communities.

As already stated in Module 2, the AI Act is risk-based, not tech-based. It focuses on how and where AI is used. Full compliance with existing regulations is mandatory, and creative professionals must assess potential data security risks by recognizing vulnerabilities in AI-powered tools and applying risk mitigation strategies to safeguard sensitive information.

Creative projects increasingly incorporate AI tools (e.g., image generators, editing software, recommendation engines) that process sensitive content, including client data, biometric info (faces, voices) or proprietary designs or concepts. The following table provides an overview of common vulnerabilities in AI-powered tools:

Vulnerability	Example	Why it is a risk
Cloud-based AI Storage	Uploading images to generative platforms	Data could be stored or reused without permission
Third-Party Plugins	AI filters or smart tagging add-ons	May extract metadata or files silently, without your knowledge
Biometric Data Use	Facial recognition or voice-based tagging	May breach GDPR if explicit consent is not obtained

AI Model Training	Using your data to “train” models	You may lose control or IP rights
Weak Access Controls	Shared accounts or unsecured uploads	Increases the risk of data leaks or unauthorized use

*Table 2. Common vulnerabilities in AI-powered tools [2]*

A risk mitigation strategy should consist of the following elements that you should apply:

1. **Know Your Tool:** Who made it? Is it reputable? Does it clearly say how it handles your data? Is it GDPR-compliant?
2. **Review Privacy Settings:** Check whether you can **opt out of data retention** and avoid tools that automatically collect data without disclosure.
3. **Avoid Uploading Sensitive Content.**
4. **Check Data Use Terms:** Can the tool use your data for training? Can you delete your uploads later?
5. **Use Secure Workflows:** Work off-line whenever it is possible, use encrypted storage for creative assets and apply two-factor authentication for cloud platforms.

In the sub-chapter 3.6 “*Assessment Criteria*” you will find a so called “*Traffic Light Checklist*” for detecting and avoiding vulnerabilities and assessing potential data security risks. This kind of ethical data management in AI-driven creative processes helps professionals to ensure compliance, build trust, and avoid reputational or legal risks. Here is a practical overview of **ethical data management practices** for responsible data collection, storage, and usage, tailored for the creative industry:

**For Responsible Data Collection,** only collect what you need. Apply the principle of data minimization (GDPR Article 5) and avoid scraping or importing datasets with unnecessary personal data. Obtain clear, informed consent and check data sources for legality. Furthermore, avoid hidden scraping or data hoarding; especially do not collect data secretly or from private spaces (e.g., locked social media accounts) without consent.

**For Secure and Fair Data Storage** encrypt sensitive data, use access controls (e.g. implement role-based access for team members), maintain clear retention policies and don’t store unregulated or anonymized personal data indefinitely. If you do not define how long data will be stored and when it will be deleted, it can result in GDPR violations and create traceability issues in creative workflows.

**For Transparent Data Usage** document AI involvement and clearly label which parts of a creative output were generated or assisted by AI (text, image, music, etc.).

In this context, it is of utmost importance to disclose data sources when requested and not to automate decisions with no human review. We strongly suggest ensuring a person checks and validates AI-assisted outcomes, especially for high-stakes outputs like hiring, design approval,

or branding. We also suggest performing regular audits and bias tests. For this purpose, you may use tools like Fairlearn or IBM AI Fairness 360 to check outputs for bias or ethical concerns, or you may involve diverse reviewers to detect cultural or visual bias. When implementing a responsible AI strategy even small teams should define how they use AI, what data sources are permitted, and how they handle IP and consent.

**Here are two practical examples of GDPR compliance, IP protection, and ethical AI data governance in design, branding, and content creation:**

### **Practical example 1: Graphic Design Studio Using AI for Logo Generation**

Scenario: A design team uses an AI tool trained in public logos to generate brand identities for clients.

- **GDPR Compliance:** No personal data is used = low GDPR risk, but it is still important to verify. Designers ensure client data (e.g., name, contact info, brand briefs) is stored securely and deleted when no longer needed.
- **IP Protection:** The team checks the AI's training data license terms to confirm it does not include copyrighted or trademarked logos. They avoid using AI-generated outputs verbatim; instead, they refine and customize for originality.
- **Ethical Data Governance:** The studio discloses to clients that an AI tool was used as part of the creative process. Clients are given rights usage terms clearly stating whether AI-generated elements are exclusive or not.

### **Practical example 2: Creative Agency Using AI to Generate Video Scripts and Ads**

Scenario: A marketing agency uses a large language model to brainstorm scripts for client ad campaigns.

- **GDPR Compliance:** No personal data is entered into the AI model. Any client-provided info is anonymized and stored in GDPR-compliant cloud services with restricted access.
- **IP Protection:** The agency does not rely solely on AI outputs — scripts are edited and customized. They confirm that generated content does not reproduce or plagiarize existing copyrighted material (e.g., lines from famous ads).
- **Ethical Data Governance:** Clients informed about which tools are used and how creative decisions are influenced by AI. They maintain content log, noting sources and authorship — important for copyright and transparency.

### 3.4. Conclusion

Artificial Intelligence offers powerful opportunities for creative professionals - from generating ideas and streamlining workflows to enhancing design and media production. However, with these capabilities come serious responsibilities, especially when handling personal data, intellectual property, and ethically sensitive content. This module explains that data privacy, security, and ethical management are not optional add-ons, but core requirements.

Creative professionals must understand and apply key data governance principles to ensure their work is legally compliant and ethically sound. This includes securing datasets, respecting IP rights, and gaining informed consent when personal or biometric data is used. It also means being transparent about when and how AI is used in the creative process, ensuring clients, collaborators, and audiences can trust the integrity of AI-assisted work.

By proactively assessing risks, using trustworthy tools, following GDPR and IP regulations, and by applying best practices for responsible data handling, creatives not only protect themselves from legal consequences - they also contribute to a more ethical and sustainable digital culture.

Moving forward, responsible data governance should be seen as an integral part of creative excellence in AI-powered environments. We recommend taking **the quiz related to this module** to check your progress. Thank you for your attention!

#### Steps to Engage with the Training Program

Step1 - Watch the Videos: Access the training videos on our platform. Each video is concise, engaging, and includes subtitles to support diverse learning needs—feel free to use them at any time of your convenience and if required.

Step 2 - Take the Quiz: After completing each video, take a short quiz available on our website. This will help you evaluate your understanding of the content and solidify the key takeaways.

Step 3 - Apply Your Learnings: Put your new skills and knowledge into practice. Use the insights you've gathered in your creative projects, focusing on AI integration, compliance, transparency, and data governance.

Step 4 - Reach Out for Support: If you have any questions or need further clarification, contact our team directly. We're here to support your learning journey and ensure you can apply the training effectively.

This flexible, user-friendly structure ensures that learners can progress at their own pace while building practical skills and confidence in using AI ethically and responsibly in their creative work.

### 3.5. Practical Exercises

The following practical exercises are designed to empower you to engage in self-driven, practice-led learning that directly connects with the module's core topics: data governance, GDPR compliance, IP protection, and ethical AI usage.

#### Practical exercise 1: Ethical Data Collection in UI/UX Design

**Scenario:** You are redesigning the UI/UX of an e-commerce website. Part of the new design includes implementing a customer feedback form.

**Your task:** Design a mock-up or written outline of the feedback form, incorporating the following ethical data management practices:

1. Include a consent checkbox explaining how customer feedback will be used.
2. Limit data fields to essentials (e.g., optional name, email, and comment).
3. Describe how you will encrypt and store the data to ensure GDPR compliance.

#### Reflection:

- How does your design build trust with users?
- Are there other privacy risks you might need to consider?

#### Helpful Guide: Ethical Data Management Checklist

*Use this as a reference when designing your feedback form:*

##### **Requirements** to ensure ethical data management:

1. **Add a checkbox for consent**, clearly stating that customer feedback will be anonymized and used only to enhance website functionality.
2. **Limit data collection** to essential fields only (e.g., optional name, email, and feedback), avoiding unnecessary personal details.
3. **Encrypt the collected data and store it securely** in compliance with GDPR, to prevent unauthorized access.

*By transparently managing data collection and respecting privacy, you create a user-friendly design while building customer trust and adhering to data governance principles.*

## Practical exercise 2: Responsible Use of AI Voice Models

**Scenario:** As a musician, you're using AI voice models to generate harmonies for a new song.

**Your task:** Write a short plan (150–200 words) describing how you would:

1. Ensure GDPR compliance when training or using AI voice models.
2. Protect intellectual property and avoid imitating real artists without consent.
3. Communicate transparently with your audience about the AI's role in your creative process (e.g., through metadata, release notes, or social media).

### Reflection:

- Would your approach change if the AI tool was third-party vs. in-house?
- What ethical concerns do you think your audience might raise?

### Helpful Guide: Ethical Use of AI Voice Models in Music Production

*Use this checklist to support your planning for responsible AI voice model usage:*

- **GDPR Compliance:** Ensure that any voice data used is either licensed or includes explicit consent from identifiable individuals. Avoid using scraped content from music platforms without authorization. If collaborating with others, clearly document data sources and obtain proper agreements.
- **IP Protection:** Use AI voice models that are either built in-house or licensed for commercial use. Edit or alter AI-generated vocals so they don't imitate real artists unless you have their approval. Understand and follow licensing terms of the tools you are using.
- **Ethical Data Governance:** Provide metadata and clear notes that indicate which vocals are AI-generated. Be transparent with your audience—use release notes, social media, or platform descriptions to disclose AI use. Keep a content log documenting the tools and processes used in production (useful for future audits or disputes).





*By managing data transparently and respectfully, you enhance user trust and meet data governance standards in your creative design.*

### 3.6. Assessment Criteria

The purpose of this assessment is to guide the ethical and lawful use of AI tools in our creative processes, ensuring compliance with legal standards and maintaining the integrity of our work. Below, we provide a so-called “*Traffic Light Checklist*” to support AI Tool Data Security. It applies to all AI-assisted activities in creative production, including design, writing, audio, video, and illustration.

Here are some suggested instructions, how you, dear learners, can use the **Checklist** to assess your self-based performance and the outcome of your exercises:

- For all evaluation criteria that are marked “**Green**”: they are safe to be used in production or client work.
- For all evaluation criteria that are marked mixed “**Green/Yellow**”: Use them with caution and apply mitigation strategies (e.g., anonymize content).
- For any “**Red**” evaluation criteria: Avoid or replace them with a compliant alternative.

 Evaluation Criteria	 Green (Safe)	 Yellow (Use with Caution)	 Red (Stop & Avoid)
<b>Data Privacy Policy</b>	Clear, GDPR-compliant, user-friendly	Vague or incomplete policy	No policy or unclear ownership of uploaded content
<b>Consent for Biometric Data</b>	Explicit, opt-in, and recorded	Implicit or not clearly stated	No consent mechanism; data reused
<b>Cloud Usage &amp; Storage</b>	No upload OR encrypted and user-controlled	Some uploads with unclear retention	Mandatory uploads with no control or deletion option
<b>Tool Transparency</b>	Clearly states data handling, processing, and AI model training use	Limited details; fine print hidden	No disclosure; data is used for model training by default
<b>IP Protection</b>	Respects user ownership; licenses are clear and non-transferable	Ownership is unclear or platform claims partial rights	Tool claims full rights or allows third-party use without notice
<b>User Access Security</b>	Requires strong passwords and 2FA	Basic login, no 2FA	Shared accounts, no access control
<b>Ability to Opt Out</b>	Can opt-out from data retention and model training	Opt-out option hidden or difficult to enforce	No opt-out; usage is mandatory





 Evaluation Criteria	 Green (Safe)	 Yellow (Use with Caution)	 Red (Stop & Avoid)
<b>Vendor Reputation</b>	Trusted, reviewed by creatives or GDPR-compliant institutions	New or unverified vendor	Known history of data misuse or security breaches

Table 3. Traffic-Light Checklist for ethical and lawful use of AI tools [3]

### 3.7. References

- [1] Jeannette zu Fürstenberg, Alexandre Momeni, Gosia Majczak, Linda Jäck and Franziska Hempelmann: An Ambitious Agenda for European AI; General Catalyst, February 2025. Link: [www.generalcatalyst.com](http://www.generalcatalyst.com)
- [2] European Artificial Intelligence Office (cnect-aioffie@ec.europa.eu), Third AI Pact webinar on AI literacy, 20.02.2025
- [3] European Commission, AI Act.  
Link: <https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai>, last time accessed on 27th of May 2025
- [4] Jure Globocnik, GDPR and AI Act: similarities and differences, October 2024  
Link: <https://www.activemind.legal/guides/gdpr-ai-act/#:~:text=Conclusion,rule%20of%20law%2C%20for%20example>, last time accessed on 27th of May 2025
- [5] Walk Me: 5 ways to master AI adoption in the workplace.  
Link: [https://www.walkme.com/content/5-ways-to-master-ai-adoption-in-the-workplace/?utm\\_campaign=search\\_generic\\_ai\\_gen&utm\\_source=google&utm\\_medium=paid&utm\\_content=182987011110&utm\\_term=ai%20business%20transformation&gad\\_source=1&gad\\_campaignid=22524225031&gbraid=0AAAAADMmSZNamIBj9XOPDCURxFC-3rr\\_K&gclid=Cj0KCQjwgIXCBhDBARIsAELC9ZgmR6mVFAWeBc1C2KGPwM3rrWfFKd9j3xrB84dxobvTUpPbVJ10DYQaAtRhEALw\\_wcB](https://www.walkme.com/content/5-ways-to-master-ai-adoption-in-the-workplace/?utm_campaign=search_generic_ai_gen&utm_source=google&utm_medium=paid&utm_content=182987011110&utm_term=ai%20business%20transformation&gad_source=1&gad_campaignid=22524225031&gbraid=0AAAAADMmSZNamIBj9XOPDCURxFC-3rr_K&gclid=Cj0KCQjwgIXCBhDBARIsAELC9ZgmR6mVFAWeBc1C2KGPwM3rrWfFKd9j3xrB84dxobvTUpPbVJ10DYQaAtRhEALw_wcB), last time accessed on 27th of May 2025
- [6] Generative AI in Creative Industries: Transforming Art, Music, and Content Creation  
Link: <https://www.qsstechnosoft.com/blog/generative-ai-134/generative-ai-in-creative-industries-transforming-art-music-and-content-creation-686#:~:text=Today%2C%20AI%20can%20study%20countless,themes%20producing%20reimagined%20traditional%20aesthetics>; last time accessed on 6th of June 2025

## About the Project

The Erasmus+ co-funded project Navigating AI Regulations: A Practical Guide (Project Number: 2024-2-DE02-KA210-VET-000287096) aims to bridge critical gaps in AI knowledge, digital skills, and EU policy awareness among trainers and freelancers in the creative industry. Grounded in an in-depth Needs Analysis conducted during the preparation stage, the project adopts a targeted approach to support the digital transformation of this dynamic sector.

The project has three core objectives:

- **Improving AI and Data Usage Competence:** By delivering a tailored training program to 57 participants, the project will enhance understanding of AI Act provisions, including risk classification, compliance, transparency, and data governance. This knowledge will empower trainers to guide young entrepreneurs in leveraging AI for business innovation while adhering to regulatory standards.
- **Enhancing Digital Skills for AI in Creativity:** Participants will gain proficiency in AI-powered tools, data analysis, and AI literacy, enabling them to integrate cutting-edge technologies into creative processes. This objective focuses on fostering innovation, improving creative workflows, and building digital resilience in the sector.
- **Boosting EU Policy and AI Act Awareness:** By increasing familiarity with EU policies and ethical frameworks, the project will ensure participants operate responsibly and in compliance with the AI Act, fostering trust and sustainable growth in the creative industry.

The project's output will directly contribute to equipping trainers and freelancers with the tools and knowledge to thrive in an AI-driven future while aligning with EU regulatory and ethical standards.

Visit our project website to discover all project information and resources: <https://regaiguide.com/>.